UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,224	01/16/2002	Mototsugu Nishioka	500.41092X00	4402

24956 7590 07/03/2007
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

\UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

MAILED

JUL 03 2007

Technology Center 2100

Application Number: 10/046,224
Filing Date: January 16, 2002
Appellant(s): NISHIOKA ET AL.

Carl I. Brundidge, Reg. No. 29,621
<u>For Appellant</u>

EXAMINER'S ANSWER

This is in response to the appeal brief filed February 7 and May 15, 2007 appealing from the Office action mailed February 7, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

Claims **23-44** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims **23-44** are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect.

The amendment after final rejection filed on 9/7/2006 has been entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is incorrect.

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner.

The rejection of claims 23-44 under 35 U.S.C. 101 is withdrawn in view of amendment.

The rejection of claims 25-27, 29, 31-34, 37-39, and 42-44 under 35 U.S.C. 112, second paragraph, because of their dependency from cancelled claims is withdrawn.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,697,488	CRAMER et al.	2-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 23, 28, 35, and 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 23, 28, 35, and 40 recite the limitations " $\alpha_1 \| \alpha_2 < q$ ". There is insufficient antecedent basis for these limitations in the claims.

Claims 24 and 40-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 24 and 40-41 recite the limitations " ciphertext and by using the secret key, $\boldsymbol{\alpha_1'}$, $\boldsymbol{\alpha_2'}$, **m'** where ". There is insufficient antecedent basis for these limitations in the claims.

Claim 30 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 30 recites the limitation "$m = D_{K'}(C)$" in page 9. There is insufficient antecedent basis for this limitation in the claim.

Claim 36 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 36 recites the limitation "transmitting ciphertext (u_1, u_2, v, **C**)" in page 13. There is insufficient antecedent basis for this limitation in the claim.

Claims 28, 40-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 28, 40-41 recite the limitation ".... = $\mathbf{D_{sk}(e)}$". There is insufficient antecedent basis for these limitations in the claims.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 23-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer.

Regarding claim 23, Cramer teaches a public-key cryptographic scheme comprising:

- a key generation step of generating a secret-key:
    - x_1 , x_2 , y_{11} , y_{12} , y_{21} , y_{22} , $z \in Z_q$ (column 7, lines 1-67)
- and a public-key:
    - G, G': finite multiplicative group $G \subseteq G'$,
    - q: prime number and the order of G,

- $g_1, g_2 \in G$ (column 6, lines 1-67, column 7, lines 1-67),
- $c= g_1\text{^}x_1\, g_2\text{^}x_2$, $d_1= g_1\text{^}y_{11}\, g_2\text{^}y_{12}$, $d_2= g_1\text{^}y_{21}\, g_2\text{^}y_{22}$, $h= g_1\text{^}z$,
- $\pi : X_1 \times X_2 \times M \rightarrow G'$: one-to-one mapping
- $\pi^{-1} : Im(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 1-67)

- where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:
  - $\alpha_1 \| \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$)
- where M is a plaintext space;
- a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ for a plaintext m ($m \in M$), calculating:
  - $u_1=g_1\text{^}r$, $u_2=g_2\text{^}r$, $e=\pi(\alpha_1, \alpha_2, m)h^r$, $v=g_1\text{^}\ \alpha_1\, c^r\ \ d_1\text{^}\,\alpha r\ d_2\text{^}\, mr$ (column 7, lines 1-67, column 8, lines 1-67)
- where $\alpha = \alpha_1 \| \alpha_2$ and transmitting (u_1, u_2, e, v) as a ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' ($\alpha_1' \in X_1$, $\alpha_2' \in X_2$, $m' \in M$) which satisfy:
  - $\pi(\alpha_1', \alpha_2', m') = e/(u_1\text{^}z)$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67) and if the following is satisfied:
  - $(g_1\text{^}\alpha_1')(u_1\text{^}(x_1+ \alpha' y_{11}+m' y_{21}))(u_2\text{^}(x_2+ \alpha' y_{12}+m' y_{22}))=v$

- outputting m' as the deciphered results (where $\alpha' = \alpha_1' \| \alpha_2'$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers ($x_1, x_2, y_1, y_2, z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45) and suggests using more elements to generate the keys (Cramer, claim 1, 11, and 20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 24, Cramer teaches a public-key cryptographic scheme comprising:

- a key generation step of generating a secret-key:
  - $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 1-67)
- and a public-key:
  - p, q: prime number where q is a prime factor of p-1,
  - $g_1, g_2 \in Z_p : ord_p(g_1) = ord_p(g_2) = q$ (column 6, lines 1-67, column 7, lines 1-67)

- $c = g_1$^x_1 g_2^x_2 mod p, $d_1 = g_1$^y_{11} g_2^y_{12} mod p, $d_2 = g_1$^y_{21} g_2^y_{22} mod p, $h = g_1$^z mod p,
- k_1, k_2, k_3 : positive constant, $10^{k1+k2} < q$, $10^{k3} < q$, $10^{k1+k2+k3} < p$ (column 7, lines 1-67)

- where a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \| \alpha_2$ where $|\alpha_1| = k_1$, $|\alpha_2| = k_2$ for a plaintext m where $|m| = k_3$ where $|x|$ is the number of digits of x), calculating: $\tilde{m} = \alpha \| K$
- selecting a random number $r \in Z_q$, calculating:
  - $u_1 = g_1^r$ mod p, $u_2 = g_2^r$ mod p, $e = \tilde{m}\, h^r$ mod p, $v = g_1$^ $\alpha_1 c^r$ d_1^ αr d_2^ mr mod p
- and transmitting (u_1, u_2, e, v) as a ciphertext (column 8, lines 1-67); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' where $|\alpha_1'| = k_1$, $|\alpha_2'| = k_2$, $|m'| = k_3$ which satisfy:
  - $\alpha_1' \| \alpha_2' \| m' = e/(u_1$^z) mod p (column 8, lines 1-67, column 9,lines 1-67, column 10, lines 1-67) and if the following is satisfied:
  - (g_1^α_1')(u_1^($x_1 + \alpha' y_{11} + m' y_{21}$))($u_2$^($x_2 + \alpha' y_{12} + m' y_{22}$))≡v (mod p)
- outputting m' as the deciphered results, where $\alpha' = \alpha_1' \| \alpha_2'$, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45) and suggests using more elements to generate the keys (Cramer, claim 1, 11, and 20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 28, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
  - $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 1-67)
- and a public-key:
  - G, G': finite multiplicative group $G \subseteq G'$,
  - q: prime number and the order of G,
  - $g_1, g_2 \in G$ (column 6, lines 1-67, column 7, lines 1-67),
  - $c= g_1$^x_1 g_2^x_2, $d_1= g_1$^y_{11} g_2^y_{12}, $d_2= g_1$^y_{21} g_2^y_{22}, $h= g_1$^z,
  - $\pi : X_1 \times X_2 \times M \rightarrow G'$: one-to-one mapping
  - $\pi^{-1} : Im(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 1-67)
  - E : symmetric encipher function (column 12, lines 1-67)

- where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:
  - $\alpha_1 \| \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$)
- where M is a key space;
- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$ for key data K ($K \in M$), calculating:
  - $u_1=g_1$^r, $u_2=g_2$^r, $e=\pi(\alpha_1, \alpha_2, K)h^r$, $v=g_1$^ $\alpha_1 c^r$ d_1^ αr d_2^ Kr (column 7, lines 1-67, column 8, lines 1-67)
- where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by:
  - $C = E_K(m)$ (column 12, lines 1-35)
- by using a symmetric cryptographic function E and key data K, and transmitting (u_1, u_2, e, v, C as the ciphertext (column 8, lines 1-67); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', K' ($\alpha_1' \in X_1$, $\alpha_2' \in X_2$, $K' \in M$) which satisfy:
  - $\pi(\alpha_1' \| \alpha_2' \| K') = e/(u_1$^z) (column 8, lines 36-67, column 9, lines 1-67, column 10, lines 1-67) and if the following is satisfied:
  - (g_1^α_1')(u_1^(x_1+ $\alpha' y_{11}$+$K' y_{21}$))(u_2^(x_2+ $\alpha' y_{12}$+$K' y_{22}$))=v where $\alpha' = \alpha_1' \| \alpha_2'$,
- executing a decipher process by:
  - $m=D_{K'}(C)$

- outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45) and suggests using more elements to generate the keys (Cramer, claim 1, 11, and 20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 29, Cramer teaches wherein the ciphertext C is generated by:

- $C = E_K(f (\alpha_1,\alpha_2) \,||\, m)$

- by using a symmetric cryptographic function E, the key data K and a publicized proper function f, it is checked whether the following is satisfied:
  - $(g_1\char`^\alpha_1')(u_1\char`^(x_1+ \alpha' y_{11}+K' y_{21}))(u_2\char`^(x_2+ \alpha' y_{12}+K' y_{22}))=v$
  - $f (\alpha_1',\alpha_2') = [D_{K'}(C)]^K$
- where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by:
  - $m= [D_{K'}(C)]^{-K}$

- where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed (column 8, lines 1-67, column 9, lines 1-67, column 12, lines 1-67).

Regarding claim 30, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
  - $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 10-19)
- and a public-key:
  - p, q: prime number, where q is a prime factor of p-1,
  - $g_1, g_2 \in Z_p$: $ord_p(g_1) = ord_p(g_2) = q$ (column 6, lines 1-67, column 7, lines 1-67)
  - $c = g_1$^x_1 g_2^x_2 mod p, $d_1 = g_1$^y_{11} g_2^y_{12} mod p, $d_2 = g_1$^y_{21} g_2^y_{22} mod p, $h = g_1$^z mod p,
  - k_1 , k_2 , k_3 : positive constant $10^{k1+k2} < q$, $10^{k3} < q$, $10^{k1+k2+k3} < p$ (column 7, lines 1-67)
  - E : symmetric encipher function (column 12, lines 1-35)
- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$, where $|\alpha_1| = k_1$, $|\alpha_2| = k_2$ for key data K $|K| = k_3$ where |x| is the number of digits of x), calculating
- $\tilde{m} = \alpha||K$ (column 7, lines 1-67, column 8, lines 1-67, column 12, lines 1-67)
- selecting a random number $r \in Z_q$, calculating:
  - $u_1 = g_1^r$ mod p, $u_2 = g_2^r$ mod p, $e = \tilde{m} h^r$ mod p, v=g_1^ $\alpha_1 c^r$ d_1^ αr d_2^ Kr mod p (column 7, lines 1-67, column 8, lines 1-67)

- and generating a ciphertext C of transmission data by:
    - $C = E_K(m)$ (column 12, lines 1-35)
- by using a symmetric cryptographic function E and the key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext (column 8, lines 1-67); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', K', where $|\alpha_1'|=k_1$, $|\alpha_2'|=k_2$, $|K'|= k_3$ which satisfy:
- $\alpha_1' || \alpha_2' || K' = e/(u_1\text{^}z) \bmod p$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)
- and if the following is satisfied:
- $(g_1\text{^}\alpha_1')(u_1\text{^}(x_1+ \alpha' y_{11}+K' y_{21}))(u_2\text{^}(x_2+ \alpha' y_{12}+K' y_{22}))\equiv v \pmod p$
- where $\alpha' = \alpha_1' || \alpha_2'$,
- executing a decipher process by:
    - $m=D_{K'}(C)$
- outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45) and suggests using more elements to generate the keys (Cramer, claim 1, 11, and 20). Therefore, it would have been obvious to one having ordinary skill in the

art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 31, Cramer teaches wherein the ciphertext C is generated by:

- $C = E_K(f(\alpha_1,\alpha_2) \,||\, m)$
- by using a symmetric cryptographic function E, the key data K and a publicized proper function f, it is checked whether the following is satisfied:
  - $(g_1 \wedge \alpha_1')(u_1 \wedge (x_1 + \alpha' y_{11} + K' y_{21}))(u_2 \wedge (x_2 + \alpha' y_{12} + K' y_{22})) \equiv v \pmod p$,
  - $f(\alpha_1',\alpha_2') = [D_{K'}(C)]^k$
- where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by:
- $m = [D_{K'}(C)]^{-K}$
- where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed (column 8, lines 1-67, column 9, lines 1-67, column 12, lines 1-67).

Regarding claim 35, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
  - $x_1, x_2, y_1, y_2, z \in Z_q$ (column 7, lines 1-67)
- and a public-key:
  - G, G': finite multiplicative group $G \subseteq G'$,
  - q: prime number the order of G,

- $g_1, g_2 \in G$ (column 6, lines 1-67, column 7, lines 1-67),
- $c= g_1\hat{}x_1\, g_2\hat{}x_2$, $d = g_1\hat{}y_1\, g_2\hat{}y_2$, $h= g_1^z$,
- $\pi : X_1 \times X_2 \times M \rightarrow \mathrm{Dom}(E)$: one-to-one mapping where Dom(E) is the domain of the function E
- $\pi^{-1} : \mathrm{Im}(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 1-67)
- H : hash function (column 12, lines 1-35)
- E : symmetric encipher function (column 12, lines 1-35)

- where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:
  - $\alpha_1 \| \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$)
- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$, calculating:
  - $u_1=g_1^r$, $u_2=g_2^r$, $v=g_1\hat{}\ \alpha_1\, c^r\ d^{\alpha r}$, $K = H(h^r)$ (column 7, lines 1-67, column 8, lines 1-67)
- where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by:
  - $C = E_K(\pi(\alpha_1, \alpha_2, m))$ (column 12, lines 1-35)
- by using a symmetric cryptographic function E; and transmitting (u_1, u_2, v, C) as the ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating
  - $K' = H(u_1^z)$

- by using the secret key, calculating from the received ciphertext, α_1', α_2', (where $\alpha_1' \in X_1$, $\alpha_2' \in X_2$) (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67) which satisfy:
    - $\pi(\alpha_1', \alpha_2', m') = D_{K'}(C)$
- if the following is satisfied:
    - $(g_1\wedge\alpha_1')(u_1\wedge(x_1+ \alpha' y_1))(u_2\wedge(x_2+ \alpha' y_2))=v$,
- where $\alpha' = \alpha_1' \,||\, \alpha_2'$,
- outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received cipher- text is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45) and suggests using more elements to generate the keys (Cramer, claim 1, 11, and 20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 36, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2, z \in Z_q$ (column 7, lines 1-67)

- and a public-key:
    - p, q: prime number (q is a prime factor of p-1),
    - $g_1, g_2 \in Z_p$: $ord_p(g_1) = ord_p(g_2) = q$ (column 6, lines 1-67, column 7, lines 1-67)
    - $c = g_1$^$x_1\ g_2$^x_2 mod p, $d = g_1$^$y_1\ g_2$^y_2 mod p, $h = g_1^z$ mod p,
    - k_1, k_2, k_3 : positive constant $10^{k1+k2} < q$, $10^{k3} < q$, $10^{k1+k2+k3} < p$ (column 7, lines 1-67)
    - H : hash function (column 12, lines 1-35)
    - E : symmetric encipher function where the domain of E is all positive integers (column 12, lines 1-35)
- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 \| \alpha_2$, where $|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where $|x|$ is the number of digits of x,
- selecting a random number $r \in Z_q$, calculating:
    - $u_1 = g_1^r$ mod p, $u_2 = g_2^r$ mod p, $v = g_1$^ $\alpha_1\ c^r\ d^{\alpha r}$ mod p, $K = H(h^r \bmod p)$
- transmitting ciphertext (u_1, u_2, v, C) (column 8, lines 1-67)
- generating a ciphertext C of transmission data m by:
    - $C = E_K(\alpha_1 \| \alpha_2 \| m)$ (column 12, lines 1-35)
- by using a symmetric cryptographic function, and transmitting (u_1, u_2, v, C) as the ciphertext (column 8, lines 1-67)
- a ciphertext reception and decipher step of calculating
    - $K' = H(u_1^z \bmod p)$

- by using the secret key, calculating from the received ciphertext, α_1', α_2', where $|\alpha_1'|=k_1$, $|\alpha_2'| = k_2$ which satisfy:
  - $\alpha_1'||\alpha_2'||m' = D_{K'}(C)$
- and if the following is satisfied:
  - $(g_1\hat{}\alpha_1')(u_1\hat{}(x_1+ \alpha'y_1))(u_2\hat{}(x_2+ \alpha'y_2))\equiv v \pmod p$
- outputting m' as the deciphered results where $\alpha' = \alpha_1' || \alpha_2'$, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45) and suggests using more elements to generate the keys (Cramer, claim 1, 11, and 20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 40, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
  - $x_1, x_2, y_1, y_2 \in Z_q$ (column 7, lines 1-67)

- sk : asymmetric cryptography decipher key (column 7, lines 1-67)

- and a public-key:
  - G : finite multiplicative group
  - q: prime number and the order of G,
  - $g_1, g_2 \in G$ (column 6, lines 65-67, column 7, lines 1-10)
  - $c= g_1$^x_1 g_2^x_2, $d= g_1$^y_1 g_2^y_2,
  - $\pi : X_1 \times X_2 \times M \rightarrow Dom(E)$: one-to-one mapping where Dom (E) is the domain of the function E
  - $\pi^{-1} : Im(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 1-67)
  - $E_{pk}(.)$: Encipher function for asymmetric cryptography (column 12, lines 1-35)
- where X_1 and X_2 are an infinite set of positive integers which satisfy:
  - $\alpha_1 \| \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$)
- where M is a plaintext space;
- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Z_q$, calculating:
  - $u_1=g_1^r$, $u_2=g_2^r$, $v=g_1$^ $\alpha_1 c^r d^{\alpha r}$ (column 7, lines 1-67, column 8, lines 1-67)
- where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by:
  - $e = E_{pk}(\pi(\alpha_1,\alpha_2,m))$ (column 12, lines 1-35)
- by using an encipher function for asymmetric cryptographic E_{pk}, and transmitting (u_1, u_2, e, v) as the ciphertext (column 8, lines 24-35); and

- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m', where $\alpha_1' \in X_1$, $\alpha_2' \in X_2$, $m' \in \mathrm{M}$ which satisfy:
  - $\pi(\alpha_1', \alpha_2', m') = D_{sk}(e)$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)
- and if the following is satisfied:
  - $(g_1\^\alpha_1')(u_1\^(x_1+ \alpha' y_1))(u_2\^(x_2+ \alpha' y_2))=v$
- where:
  - $\alpha' = \alpha_1' \,||\, \alpha_2'$
- outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45) and suggests using more elements to generate the keys (Cramer, claim 1, 11, and 20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 41, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
  - $x_1, x_2, y_1, y_2 \in Z_q$ (column 7, lines 1-67)
  - sk : asymmetric cryptography decipher key (column 7, lines 1-67)
- and a public-key:
  - p, q: prime number where q is a prime factor of p-1
  - $g_1, g_2 \in Z_p$: $ord_p(g_1) = ord_p(g_2) = q$ (column 6, lines 1-67, column 7, lines 1-67)
  - $c = g_1$^x_1 g_2^x_2 mod p, $d = g_1$^y_1 g_2^y_2 mod p,
  - k_1 , k_2 : positive constant $10^{k1+k2} < q$
  - $E_{pk}(.)$: encipher function for asymmetric cryptography where the domain is all positive integers) (column 12, lines 1-35)
- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 \| \alpha_2$, where $|\alpha_1| = k_1$, $|\alpha_2| = k_2$ where $|x|$ is the number of digits of x, selecting a random number $r \in Z_q$, calculating:
  - $u_1 = g_1^r$ mod p, $u_2 = g_2^r$ mod p, $v = g_1$^ $\alpha_1 c^r d^{\alpha r}$ mod p
- generating a ciphertext C of transmission data m (positive integer) by:
  - $e = E_{pk}(\alpha_1 \| \alpha_2 \| m)$ (column 12, lines 1-35)
- by using the secret key, and transmitting (u_1, u_2, e, v) as the ciphertext (column 8, lines 1-67); and

- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' where $|\alpha_1'|=k_1$, $|\alpha_2'|=k_2$, m' is a positive integer which satisfy:
  - $\alpha_1' || \alpha_2' || m' = D_{sk}(e)$ (column 8, lines 36-67, column 9,lines 1-67, column 10, lines 1-67)
- and if the following is satisfied:
  - $(g_1\verb|^|\alpha_1')(u_1\verb|^|(x_1+ \alpha' y_1))(u_2\verb|^|(x_2+ \alpha' y_2))=v \pmod p$,
- where
  - $\alpha' = \alpha_1' \, || \, \alpha_2'$
- outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1, x_2, y_1, y_2, $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2; e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45) and suggests using more elements to generate the keys (Cramer, claim 1, 11, and 20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claims 25, 32, 37, and 42, Cramer teaches wherein the public-key is generated by a receiver and is made public (columns 1-3).

Regarding claims 26 and 33, Cramer teaches wherein in said ciphertext transmission step, the random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, and $r \in Z_q$ are selected beforehand and the following is calculated and stored beforehand: $u_1=g_1^r$, $u_2=g_2^r$, h^r, g_1^α_1 c^r d_1^αr (column 7, lines 1-67, column 8, lines 1-67).

Regarding claims 27 and 34, Cramer teaches wherein in said ciphertext transmission step, the random numbers α_1, α_2 where $|\alpha_1|= k_1$, $|\alpha_2|= k_2$, and $r \in Z_q$ are selected beforehand and the following is calculated and stored beforehand: $u_1=g_1^r$ mod p, $u_2=g_2^r$ mod p, h^rmod p, g_1^α_1 c^r d_1^αr mod p (column 7, lines 40-67, column 8, lines 1-22).

Regarding claims 38 and 43, Cramer teaches wherein in said ciphertext transmission step, the random numbers α_1 , α_2, where $\alpha_1 \in X_1$, $\alpha_2 \in X_2$ and $r \in Z_q$ are selected beforehand and the u_1, u_2, e, and v (u_1, u_2, and v) are calculated and stored beforehand (column 7, lines 40-67, column 8, lines 1-22).

Regarding claims 39 and 44, Cramer teaches wherein in said ciphertext transmission step, the random numbers α_1 , α_2 ($|\alpha_1|= k_1$, $|\alpha_2| = k_2$), and $r \in Z_q$ are selected beforehand and the u_1, u_2, e, and v (u_1, u_2, and v) are calculated and stored beforehand (column 7, lines 40-67, column 8, lines 1-22).

(10) Response to Argument

A. 35 USC §112, second paragraph rejection of claim 25-27, 29, 31-34, 37-39 and 42-44

Regarding the remaining claims (independent claims 23, 24, 28, 30, 35, 36, 40 and 41) Appellant has failed to address the insufficient antecedent basis issues raised on the previous office action, i.e. the independent claims list a number of elements that are not defined and are not properly tied to the body of the claim, rendering the claims indefinite. Claim 23's limitation of satisfying "$\alpha_1 \| \alpha_2 < q$" is indefinite because there is insufficient antecedent basis, the elements are not defined, it is not clear how those elements are generated or obtained and / or what they are intended to be, thus the metes and bounds of the claim are not definite. Claims 23, 24, 28, 30, 35, 36, 40 and 41 recite the limitations "**a key generation step of generating a secret-key:**" and "**a public-key:**" with a list of undefined elements in between without a relation of how are they being used to generate a key or how are they obtained/selected. The relationship between the elements listed and how they are used to produce a key is not clear, i.e. claim 23 states "a key generation step of generating a secret-key: x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, $z \in Z_q$ and a public-key: G, G': finite multiplicative group $G \subseteq G'$, q: prime number and the order of G, $g_1, g_2 \in G$, $c= g_1$^$x_1\, g_2$^x_2, $d_1= g_1$^$y_{11}\, g_2$^y_{12}, $d_2= g_1$^$y_{21}\, g_2$^y_{22}, $h= g_1$^z, $\pi : X_1 \times X_2 \times M \rightarrow G'$: one-to-one mapping, $\pi^{-1} : Im(\pi) \rightarrow X_1 \times X_2 \times M$", the metes and bounds of patent protection being sought is not clearly defined. Appellant's arguments are not persuasive. Examiner contrasts the language found in the instant

application with the language found in the prior art's claims, where the variables are clearly defined. A clear definition of the variables would overcome this 112 rejection.

Similar argument applies to the remaining independent claims.

C.35 USC §103(a) rejection of claims 23-44

In response to Appellant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., hash function or hash value not being used, the elements are not defined, thus the elements are broadly interpreted as values/numbers, a hash value being of a narrower nature – page 18 of the Appeal Brief) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification (namely, that the values are not hash values or hash functions) are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Even if a hash value or hash function were not used and claimed, Cramer teaches that the use of a hash function can be omitted (col.9,lines 60-67). Appellant's arguments are not persuasive.

Regarding Appellant's argument that the instant application uses 2 more elements than Cramer, such argument is not persuasive since Cramer expressly claims **"choosing at least a first, second, and third..."** (Cramer, claim 1) which clearly suggests using more elements that the ones disclosed, since Cramer already recognizes the benefits and drawbacks of heavier computations in the calculation of the keys, i.e. heavier computations would make it more difficult for an unauthorized entity to

access encrypted data while lighter computations would be faster to compute (Cramer, col. 1, lines 40-60). Appellant's arguments are not persuasive.

Regarding Appellant's argument that Cramer does not teach "d1" and "d2" (pages 20-21), Examiner respectfully submits that Cramer teaches "d_i" (Cramer, section V, column 9), thus "d_i" can change and varies. Appellant's arguments are not persuasive.

In response to Appellant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., k is 2 and kept small – page 22 of the Appeal Brief) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Appellant's arguments are not persuasive.

i. Independent Claim 23

Regarding Appellant's argument that the instant application uses 2 more elements than Cramer, such argument is not persuasive since Cramer expressly claims **"choosing at least a first, second, and third..."** (Cramer, claim 1) which clearly suggests using more elements that the ones disclosed, since Cramer already recognizes the benefits and drawbacks of heavier computations in the calculation of the keys, i.e. heavier computations would make it more difficult for an unauthorized entity to access encrypted data (Cramer, col. 1, lines 40-60). Appellant's arguments are not persuasive.

Regarding Appellant's argument that Cramer does not disclose a specific calculation (page 25), Examiner respectfully submits that Cramer expressly claims and teaches performing calculations with the specific elements to obtain keys and decrypted data (claims 1 and 11, col. 11, lines 43-60), adding / subtracting / raising to the power / or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the instant application form the prior art (Cramer). Appellant's arguments are not persuasive.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

ii. Independent Claim 24

Regarding Appellant's argument that the instant application uses 2 more elements than Cramer, such argument is not persuasive since Cramer expressly claims **"choosing at least a first, second, and third..."** (Cramer, claim 1) which clearly suggests using more elements that the ones disclosed, since Cramer already recognizes the benefits and drawbacks of heavier computations in the calculation of the keys, i.e. heavier computations would make it more difficult for an unauthorized entity to

access encrypted data (Cramer, col. 1, lines 40-60). Appellant's arguments are not persuasive.

iii. Independent Claim 28

Regarding Appellant's argument that the instant application uses 2 more elements than Cramer, such argument is not persuasive since Cramer expressly claims **"choosing at least a first, second, and third..."** (Cramer, claim 1) which clearly suggests using more elements that the ones disclosed, since Cramer already recognizes the benefits and drawbacks of heavier computations in the calculation of the keys, i.e. heavier computations would make it more difficult for an unauthorized entity to access encrypted data (Cramer, col. 1, lines 40-60). Appellant's arguments are not persuasive.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Contrary to Appellant's assertion that Cramer teaches away from adding additional elements, Examiner respectfully points Appellant's attention to Cramer's claims 1, 11, and 20, where the use of more elements is suggested ("**choosing at**

least", contrast such language with "**choosing at most**", where it would be limiting to some predetermined number of elements). Appellant's arguments are not persuasive.

iv. Independent Claim 30

Regarding Appellant's argument that the instant application uses 2 more elements than Cramer, such argument is not persuasive since Cramer expressly claims **"choosing at least a first, second, and third..."** (Cramer, claim 1) which clearly suggests using more elements that the ones disclosed, since Cramer already recognizes the benefits and drawbacks of heavier computations in the calculation of the keys, i.e. heavier computations would make it more difficult for an unauthorized entity to access encrypted data (Cramer, col. 1, lines 40-60). Appellant's arguments are not persuasive.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Contrary to Appellant's assertion that Cramer teaches away from adding additional elements, Examiner respectfully points Appellant's attention to Cramer's claims 1, 11, and 20, where the use of more elements is suggested ("**choosing at**

least", contrast such language with "**choosing at most**", where it would be limiting to some predetermined number of elements). Appellant's arguments are not persuasive.

v. Independent Claim 35

Regarding Appellant's argument that Cramer does not expressly teach "$v=g_1$^ α_1 c^r $d^{\alpha r}$, $K = H(h^r)$", Examiner respectfully submits that Cramer provides the teachings of using a hash function and generating a verification value by means other than modular arithmetic (col. 7, lines 60-67, col. 8, lines 1-10), and using a broad but reasonable interpretation of the claim limitations, Cramer discloses on column 12 generating K as a value of a hash function is disclosed (Cramer, col. 12, lines 13-27). Appellant's arguments are not persuasive.

Regarding Appellant's argument that Cramer does not calculate K, Examiner respectfully submits that as loosely defined, K, can be interpreted as a hash value, which Appellant has already admitted Cramer uses (Appeal Brief, pages 20-21).

In response to Appellant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., hash function or hash value not being used, the assumptions based upon – page 18 of the Appeal Brief) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Even if a hash value or hash function were not used and claimed, Cramer teaches that the use of a hash function can be omitted (col.9,lines 60-67). Appellant's arguments are not persuasive.

vi. Independent Claim 36

Regarding Appellant's argument that the instant application uses 2 more elements than Cramer, such argument is not persuasive since Cramer expressly claims **"choosing at least a first, second, and third..."** (Cramer, claim 1) which clearly suggests using more elements that the ones disclosed, since Cramer already recognizes the benefits and drawbacks of heavier computations in the calculation of the keys, i.e. heavier computations would make it more difficult for an unauthorized entity to access encrypted data (Cramer, col. 1, lines 40-60). Appellant's arguments are not persuasive.

Regarding Appellant's argument that Cramer does not disclose a specific calculation (page 49), Examiner respectfully submits that Cramer expressly claims and teaches performing calculations with the specific elements to obtain keys and decrypted data (claims 1 and 11, col. 11, lines 43-60), adding / subtracting / raising to the power / hash function / or performing a mod operation without clearly defining what the numbers are do not patentably distinguish the instant application form the prior art (Cramer). Appellant's arguments are not persuasive.

Regarding Appellant's argument that Cramer does not calculate K, Examiner respectfully submits that as loosely defined, K, can be interpreted as a hash value, which Appellant has already admitted Cramer uses (Appeal Brief, pages 20-21).

vii. Independent Claim 40

Regarding claim 40, Cramer teaches a verification cipher-number v to be used to verify the encrypted value (col. 7, lines 60-67, col. 8, lines 1-22). Appellant's arguments

are not persuasive. Regarding Appellant's argument that Cramer does not expressly teach "transmitting (u_1, u_2, e, v)", Examiner respectfully submits that Cramer provides the teachings of using module arithmetic to generate the verification value (col. 7, lines 60-67, col. 8, lines 1-10), and using a broad but reasonable interpretation meets the claim limitations. Appellant's arguments are not persuasive.

Contrary to Appellant's arguments, Cramer in fact transmits (u_1, u_2, e, v) (col. 11, lines 40-60). Appellant's arguments are not persuasive.

viii. Independent Claim 41

Regarding Appellant's argument that the instant application uses 2 more elements than Cramer, such argument is not persuasive since Cramer expressly claims **"choosing at least a first, second, and third..."** (Cramer, claim 1) which clearly suggests using more elements that the ones disclosed, since Cramer already recognizes the benefits and drawbacks of heavier computations in the calculation of the keys, i.e. heavier computations would make it more difficult for an unauthorized entity to access encrypted data (Cramer, col. 1, lines 40-60). Appellant's arguments are not persuasive.

Regarding Appellant's argument that Cramer does not expressly teach '$v=g_1$^ α_1 c^r $d^{\alpha r}$ mod p", Examiner respectfully submits that Cramer provides the teachings of using module arithmetic to generate the verification value (col. 7, lines 60-67, col. 8, lines 1-10), and using a broad but reasonable interpretation meets the claim limitations. Appellant's arguments are not persuasive.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

David García Cervetti

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron, SPE

Benjamin Lanier